UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,926	10/29/2001	Hiroshi Maruyama	JP920000300US1	1476

7590 03/17/2006

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/017,926	MARUYAMA ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *18 and 20* is/are allowed.

6)☒ Claim(s) *1-2, 5-6, 7-8, 10-17, 19, 21-22, and 25-28* is/are rejected.

7)☐ Claim(s) *3,4,9 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/15/2005 has been entered.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 5, 7-8, 10-15, 17, 19, 21-22, 25, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein USPN 6,453,416 B1 in view of Matyas et al. (herein after Matyas, USPN 4,206,315).

Regarding claims 1, 7, 15, 17, 19, 21-22, 25, and 27, Epstein teaches a proxy server/system/method/medium for relaying communications between applications and for performing an additional process comprising:

a key manager for managing multiple keys used to generate a digital signature to be provided for a message document that is exchanged between said applications, wherein each of

said multiple keys is used to sign messages having particular message contents, wherein each of said multiple keys is used to sign messaged having particular message contents (col. 4 lines 14-23);

a signature key determiner for extracting said message document from a predetermined application, and for, based on said message document, determining a key, wherein said content do not include any digital signature data (col. 6 lines 12-67; *proxy signature key is determined based on the received document and wherein the document do not include signature information)*; and

a signature generator for providing a digital signature for said message document by using said key that is obtained from said key manager based on a determination made by said signature key determiner, and for transmitting said message document with said digital signature to a destination application (col. 2 lines 39-65).

Epstein fails to explicitly teach determining a key from said multiple keys that is to be used to provide a digital signature,

However Matyas discloses a signature key table and selecting signature keys from the table to generate digital signature (fig. 1 and fig. 2).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Matyas within the system of Epstein because it would generate a signature using a selected and required signature key. One would have been motivated to modify the teachings of key selection because it would provide a digital signature for documents using different user signature keys.

Regarding claims 10, 11, and 23-24, they have the same limitations as claim 1 above and they have been rejected under the same rational as claim 1. And further Epstein teaches obtaining a public key for verifying intercepted message or communication and verifying digital signature provided for the message using public key to determine if the message is authorized (col. 7 lines 52-62).

Regarding claim 2, Matyas further teaches the proxy server, wherein said key manager sets multiple key selection rules for obtaining said key, and only when said key selection rules are satisfied can said signature generator obtain said key (col. 4 lines 17-60).

Regarding claim 5, Epstein further discloses the proxy server, further comprising: a log manager for storing said message document with a digital signature provided by said signature generator, and for managing a log (col. 6 lines 39-49).

Regarding claim 8, Matyas further teaches the digital signature system, wherein said proxy server permits a key used to provide a digital signature to be changed in accordance with the contents of a message document; and wherein said proxy server sets key selection rules for said key and permits digital signature using said key when said key selection rules have been satisfied (fig. 1-2 and col. 3 lines 11-51).

Regarding claim 12, Epstein further teaches the network system, wherein, when said application of said local group transmits a message document, said proxy server stores the message

document with a digital signature in a log, and manages said log; wherein, when said application of said local group receives a message document from a different group, said proxy server stores in a log a message document authenticated by a verification of a digital signature, and manages said log; and wherein, at a predetermined timing, said proxy server compares the transmission log with the reception log for the same message document, and authorizes communication (col. 6 lines 39-49).

Regarding claim 13, Epstein further teaches the network system, wherein said proxy server compares signature information for a digital signature concerning the same message document (col. 6 lines 12-49).

Regarding claim 14, Epstein further teaches the network system, wherein said proxy server compares hash values used for providing a digital signature for the same message document (col. 6 lines 12-49 and col. 7 lines 52-62).

4. Claims 6, 16, 26, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein USPN 6,453,416 B1 in view of Matyas et al. (herein after Matyas, USPN 4,206,315) and further in view of Spelman et al. (herein after Spelman, 5,680,458).

Regarding claims 16, 26, and 28, it has the same limitations as claim 10 above and it has been rejected under the same rational as claim 10. Claim 16 recites more limitations that is the combination of Epstein and Matyas fails to disclose, such as:

accepting a message document with a digital signature that uses a replacement key, when said digital signature on said received message document has been provided by using said replacement key for an original key that is determined in accordance with the type of said message document; and

receiving a message document, after said message document signed using said replacement key has been accepted, with a digital signature that used said original key.

However Spelman teaches accepting a message document with a digital signature that uses a replacement key, when said digital signature on said received message document has been provided by using said replacement key for an original key that is determined in accordance with the type of said message document (Spelman col. 6 lines 47-63; *replacement public key that corresponds to the replacement private key and the digital signature that is generated using the central authority's replacement private key is verified and accepted along with the message*); and

receiving a message document, after said message document signed using said replacement key has been accepted, with a digital signature that used said original key (col. 3 lines 19-64 and fig. 2).

Therefore it would have been obvious to one having ordinary skill in the art at he time of the invention was made to employ the teachings of Spelman within the combination system of Epstein and Matyas because it would allow to effectively and efficiently provide the replacement key so that the public can trust a valid key (Spelman col. 1 lines 52-57). One skilled in the art at the time of the invention was made would modify these teachings to receive a message document with a digital signature that used said original key after the message document signed using said

replacement key has been accepted because it would additionally provide a digital signature that uses a private key.

Regarding claim 6, Epstein and Matyas disclose all the subject matter as described above. Epstein and Matyas fail to disclose replacement key log manager storage.
However Spelman discloses replacement key log manager storage (col. 2 lines 66-col. 3 lines 18)

Allowable Subject Matter

5. Claims 18 and 20 are allowed.

6. Claims 3, 4, 9, and 29, are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 10, 11, 16, 17, and 19 would be allowable if rewritten or amended to overcome the rejection(s), set forth in this Office action, and to include all the limitation as recited in claim 1, as objected for being dependent claims for claim 1, and any intervening claims.

7. The following is a statement of reasons for the indication of allowance:

Claims 18 and 20 are allowed.

Claims 18 and 20: Prior art of record neither alone nor in combination teach a proxy server/medium/apparatus comprising a process for selecting one of a plurality of keys used to provide a digital signature for a message document in accordance with a type of message document transmitted from a predetermined application, wherein content do not include any digital signature data and wherein each of said plurality of keys is used to sign messages having

particular message contents; a process for providing said digital signature for said message document using said key that is selected, and for employing a predetermined replacement key to provide said digital signature for said message document, when key selection rules for said key used to provide a digital signature for said message document, when key selection rules for said key used to provide a digital signature for said message document have not been satisfied; and a process for employing said key to provide again a digital signature for said message document, when said key selection rules for said key are satisfied after said digital signature has been provided using said replacement key.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

E.S.
March 13, 2006